



09-17-04 IFW  
Express Mailing Label No. EV 380179533 US

Docket No. 971-28-001

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants: O. ATSUMI et al.

Serial No. 10/692,483

Art Unit: 2131

Filing Date: October 23, 2003

For: RANDOM NUMBER GENERATION APPARATUS

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

TRANSMITTAL

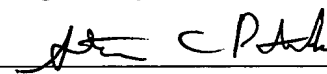
Sir:

Transmitted herewith is a certified copy of the priority document in accordance with 35 USC 365(c).

If any additional fee is required, charge Deposit Account No. 11-1580. A duplicate of this transmittal is attached.

Respectfully submitted,

September 15, 2004

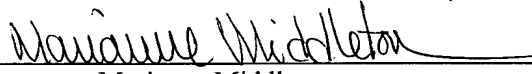
  
\_\_\_\_\_  
Steven C. Patrick  
Registration No. 40,341  
Attorney for Applicant

KOPPEL, JACOBS, PATRICK & HEYBL  
555 St. Charles Drive, Suite 107  
Thousand Oaks, California, 91360  
Telephone: (805) 373-0060

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service via Express mail in an envelope addressed to: Commissioner of Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

9/15/04  
\_\_\_\_\_  
Date

  
\_\_\_\_\_  
Marianne Middleton



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. No. : 10/692,483  
Applicants : O. Atsumi et al.  
Filed : October 23, 2003  
TC/A.U. : 2131  
Docket No. : 971-28-001  
Title: RANDOM NUMBER GENERATION APPARATUS

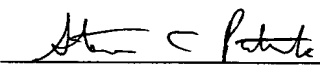
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

SUBMISSION OF CERTIFIED COPY OF PRIORITY DOCUMENT IN  
ACCORDANCE WITH 35 USC 365(c)

Sir:

Please find enclosed a certified copy of the priority document - Japanese patent application no. 163428/2001, filed in Japan on April 24, 2001 - cited for the patent application identified above.

Respectfully submitted,

  
Steven C. Patrick  
Registration No. 40,341  
Attorney for Applicant

September 15, 2004

KOPPEL, JACOBS, PATRICK & HEYBL  
555 St. Charles Drive, Suite 107  
Thousand Oaks, California 91360  
(805) 373-0060

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されて  
る事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed  
with this Office.

出 願 年 月 日      2 0 0 1 年    4 月 2 4 日  
Date of Application:

出 願 番 号      特 願 2 0 0 1 - 1 6 3 4 2 8  
Application Number:  
[T. 10/C]:      [ J P 2 0 0 1 - 1 6 3 4 2 8 ]

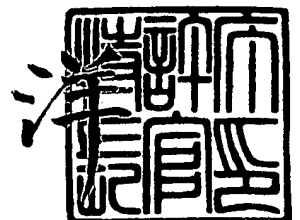
願      人  
Applicant(s):      株式会社三技協  
                         株式会社サンテクト

CERTIFIED COPY OF  
PRIORITY DOCUMENT

2 0 0 4 年    8 月    9 日

特 許 庁 長 官  
Commissioner,  
Japan Patent Office

小 川



BEST AVAILABLE COPY

出 証 番 号    出 証 特 2 0 0 4 - 3 0 7 0 9 4 7

【書類名】 特許願

【整理番号】 SA01-02

【あて先】 特許庁長官殿

【提出日】 平成13年 4月24日

【国際特許分類】 H04I 19/28

【発明者】

    【住所又は居所】 神奈川県相模原市北里 2 - 1 7 - 2 7

    【氏名】 三田 二三夫

【発明者】

    【住所又は居所】 神奈川県相模原市上鶴間 2 - 8 - 3 8

    【氏名】 渥美 治

【特許出願人】

    【識別番号】 595095353

    【氏名又は名称】 株式会社三技協

【特許出願人】

    【識別番号】 500459292

    【氏名又は名称】 株式会社サンテクト

【代理人】

    【識別番号】 100071098

    【弁理士】

    【氏名又は名称】 松田 省躬

【手数料の表示】

    【予納台帳番号】 039240

    【納付金額】 21,000円

【提出物件の目録】

    【物件名】 明細書 1

    【物件名】 図面 1

    【物件名】 要約書 1

【書類名】 明細書

【発明の名称】 乱数発生装置

【特許請求の範囲】

【請求項 1】 物理的な雑音を測定してランダム雑音を発生するランダム雑音発生手段と、

このランダム雑音を波形整形してランダムパルス波を生成するランダムパルス波生成手段と、

このランダムパルス波を一定周期のクロックでサンプリングしてサンプル値のオン・オフをパルス符号とする一定周期の 2 値パルス列に変換する 2 値パルス列変換手段と、

この 2 値パルス列の極性を一定周期おきに反転させて所定の単位符号長における 1 / 0 符号の出現バランスを平滑化する 2 値パルス列符号平滑化手段と、  
を備え、

前記 2 値パルス列符号の乱数列を発生してなる乱数発生装置。

【請求項 2】 前記ランダム雑音の発生間隔をパルスのオン・オフ時間として前記ランダムパルス波を生成してなる請求項 1 記載の乱数発生装置。

【請求項 3】 前記ランダム雑音発生手段を複数用いて合成したランダム雑音を前記ランダムパルス波生成手段に入力して前記ランダムパルス波のオン・オフの発生頻度を増大させてなる請求項 1 記載の乱数発生装置。

【請求項 4】 前記ランダムパルス波生成手段を対数増幅器とコンパレータおよび単安定マルチバイブレータまたはトグルフリップフロップで構成してなる請求項 1 記載の乱数発生装置。

【請求項 5】 前記 2 値パルス列符号平滑化手段を前記クロックの周波数を 1 / 2 に分周する 1 / 2 分周器とマルチプレクサまたは X O R ゲートで構成してなる請求項 1 記載の乱数発生装置。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、情報セキュリティ用の I D パスワードや各種暗号鍵などに使用する

ための乱数を発生する乱数発生装置に関する。

#### 【0002】

##### 【発明が解決しようとする課題】

IDパスワードや各種暗号鍵などの安全性を高めるには、1／0の出現確率が各々1／2の等確率で、各ビットが他と独立してビット間に相関のない真正乱数を使用する必要がある。

真正乱数は、実際にサイコロやコインを振るわけにもいかないので、電氣的な雑音の電圧変化を測定するなどの物理乱数を用いて生成することが多いが、物理乱数をそのまま用いても真正乱数とはならない。

#### 【0003】

物理乱数のビット列は、1／0が無規則に出現するが、1／0の出現バランスは不確定さを持つためインバランスとなる。

そのため、物理乱数のインバランスを解消する方法として、出力パルス列の積分値を乱数生成側にフィードバックして雑音レベルを制御したり、出力パルス列をシフトレジスタに入力してパラレル変換したパルス列の論理和を求めて乱数を生成するなどの方法が提案されている。

ところが、いずれの方法も偶然性に支配される要素が多いため、確実に1／0の出現バランスを等確率にすることは困難であった。

#### 【0004】

そこで本発明は、偶然性に支配されることなく物理乱数のインバランスを解消して確実に1／0の出現バランスを等確率にできる乱数発生装置を提供することを目的になされたものである。

#### 【0005】

##### 【課題を解決するための手段】

かかる目的を達成するために、本発明は以下のように構成した。

すなわち、請求項1の発明は、物理的な雑音を測定してランダム雑音を発生するランダム雑音発生手段と、

このランダム雑音を波形整形してランダムパルス波を生成するランダムパルス波生成手段と、

このランダムパルス波を一定周期のクロックでサンプリングしてサンプル値のオン・オフをパルス符号とする一定周期の2値パルス列に変換する2値パルス列変換手段と、

この2値パルス列の極性を一定周期おきに反転させて所定の単位符号長における1/0符号の出現バランスを平滑化する2値パルス列符号平滑化手段と、  
を備え、

前記2値パルス列符号の乱数列を発生してなる乱数発生装置である。

#### 【0006】

請求項2の発明は、前記ランダム雑音の発生間隔をパルスのオン・オフ時間として前記ランダムパルス波を生成してなる請求項1記載の乱数発生装置である。

請求項3の発明は、前記ランダム雑音発生手段を複数用いて合成したランダム雑音を前記ランダムパルス波生成手段に入力して前記ランダムパルス波のオン・オフの発生頻度を増大させてなる請求項1記載の乱数発生装置である。

請求項4の発明は、前記ランダムパルス波生成手段を対数増幅器とコンパレータおよび単安定マルチバイブレータまたはトグルフリップフロップで構成してなる請求項1記載の乱数発生装置である。

請求項5の発明は、前記2値パルス列符号平滑化手段を前記クロックの周波数を1/2に分周する1/2分周器とマルチプレクサまたはXORゲートで構成してなる請求項1記載の乱数発生装置である。

#### 【0007】

##### 【発明の実施の形態】

以下に図面を参照して本発明の実施の形態について説明する。

図1に、本発明を実施した乱数発生装置のブロック図を示す。

また、各ブロックの信号波形とそのタイミングチャートを図2に示す。

乱数発生装置は、雑音源1が発生する周期性のないランダム雑音nを波形整形回路2に入力してランダムパルス波p1を生成する。

#### 【0008】

次に、ランダムパルス波p1と発振器3のクロックc1をサンプル&ホールド回路4に入力して一定周期の2値パルス列p2を生成する。

そして、2 値パルス列 p 2 とクロック c 1 を分周器 5 で  $1/2$  に分周した  $1/2$  分周クロック c 2 をスイッチング回路 6 に入力して 2 値パルス列 p 2 の極性を 1 周期おきに反転させ、 $1/0$  符号の出現バランスを平滑化した平滑 2 値パルス列 p 3 を出力する。

#### 【0009】

雑音源 1 は、熱雑音、ショット雑音、電子なだれなどによる白色雑音を物理的な雑音の発生源とする。

#### 【0010】

波形整形回路 2 は、ランダム雑音 n を対数増幅回路で所定の電圧レベルに増幅し、これをコンパレータに入力してトリガレベル以上の雑音波形をトリガパルスとして取り出す。

そして、これを単安定マルチバイブレータに入力して外付けの C R によって決まる所定のパルス幅を有するランダムパルス波 p 1 を生成する。

このときのパルス幅は、サンプリング定理によりクロック c 1 のパルス幅の 2 倍以上に設定する。

また、このときのトリガパルスはランダムパルス波 p 1 の立ち上がり、もしくは立ち下りのエッジ部分となり、トリガパルスの幅が長くなったり短くなったりしても一定のパルス幅を得ることができる。

#### 【0011】

ランダム雑音 n の発生間隔にばらつきがある場合は、トリガパルスを T 入力のたびに Q 出力が反転する T-F F 2 進カウンタに入力してトリガパルスの発生間隔をパルスのオン・オフ時間とするランダムパルス波 p 1 を生成してもよい。

これにより、ランダムパルス波 p 1 のオン・オフ時間の割合を均等にすることができる。

#### 【0012】

乱数の発生を高速化する場合は、複数の同一あるいは多種類の雑音源 1 の出力を合成し、波形整形回路 2 を介してサンプル&ホールド回路 4 に入力する。

これにより、ランダム雑音 n の発生頻度を増大させてランダムパルス波 p 1 のオン・オフの切換えを頻繁にする。



この場合、ランダム雑音  $n$  の発生頻度に応じてクロック  $c_1$  の周期を短くし、クロック  $c_1$  の周期に応じてランダムパルス波  $p_1$  のパルス幅を適正な長さに調節する必要がある。

### 【0 0 1 3】

サンプル&ホールド回路 4 は、図 3 に示すように、FF を 2 個使用して C 入力 は入力側の FF に直接、出力側の FF にはインバータを介して反転したクロック  $c_1$  を供給する。

これにより、C 入力のアップエッジで入力側の FF に記憶された D 入力のランダムパルス波  $p_1$  のオン・オフは、出力側の FF の C 入力が “0” なのでそのまま出力側の FF の Q 出力に転送され、C 入力のダウンエッジでは出力側の FF の C 入力がアップエッジになるので Q 出力を保持し、次の C 入力のアップエッジまでその状態を変えずにいる。

このため、C 入力のアップエッジでランダムパルス波  $p_1$  のオン・オフ状態を記憶した 2 値パルス列  $p_2$  がクロック  $c_1$  の  $1/2$  の周期でクロック  $c_1$  に同期して出力される。

### 【0 0 1 4】

分周器 5 は、T-FF の T 入力にクロック  $c_1$  を 2 発入力するたびに Q 出力を元の状態に戻してクロック  $c_1$  を  $1/2$  に分周する。

あるいは、図 4 に示すように、D-FF の反転 Q 出力を D 入力に接続して D-FF を T-FF として動作させてもよい。

このとき、反転 Q 出力が次の D 入力となるので、C 入力のあるたびに Q 出力が反転する。

### 【0 0 1 5】

スイッチング回路 6 は、図 5 に示すように、2 個の AND ゲートと OR ゲートおよびインバータを組み合わせたマルチプレクサで構成し、 $1/2$  分周クロック  $c_2$  を制御入力として制御入力の “1” または “0” により 2 値パルス列  $p_2$  の正相出力と逆相出力のいずれか一方を選択して平滑 2 値パルス列  $p_3$  を出力する。

あるいは、図 6 に示すように、2 値パルス列  $p_2$  と  $1/2$  分周クロック  $c_2$  を

XORゲートに入力して両者を排他的論理和で加算し、 $1/2$ 分周クロック  $c_2$  の  $1/0$  に同期して2値パルス列  $p_2$  の符号を1周期毎に正逆転させて平滑2値パルス列  $p_3$  を出力してもよい。

なお、実施例では $1/2$ 分周により正相出力と逆相出力を切換える方法をとっているが、分周度合いを高めて所定の単位符号長における  $1/0$  符号の出現バランスを平滑化する方法も実施可能である。

#### 【0016】

##### 【発明の効果】

以上説明したように、本発明の乱数発生装置は、ランダム雑音を波形整形してランダムパルス波を生成し、これをクロックでサンプリングして一定周期の2値パルス列に変換し、その極性を一定周期おきに反転させて2値パルス列符号の乱数列を発生する。

従って、本発明によれば、通常、2値パルス列の  $1/0$  の出現バランスは、雑音の発生頻度に左右されるのでインバランスとなるが、このように2値パルス列の極性を一定周期おきに反転させると、符号配列のインバランス性が平滑化されて確実に  $1/0$  の出現確率がおのおの  $1/2$  に近い2値パルス列が得られる。

#### 【0017】

例えば、2値パルス列を“01100011001110000100”とすると、 $1/0$  の出現確率はおのおの  $8/20$  と  $12/20$  となり“0”に偏っているが、その極性を1周期おきに反転させると“00110110011011010001”となり、 $1/0$  の出現確率はおのおの  $10/20$  と  $10/20$  で、 $1/2$  あるいはそれに近い値となる。

#### 【0018】

また、本発明の乱数発生装置は、ランダム雑音の発生間隔をパルスのオン・オフ時間としてランダムパルス波を生成する。

従って、本発明によれば、通常、ランダムパルス波のオン・オフ時間の割合は、雑音の発生頻度に左右されるのでいずれか一方に偏るが、このようにランダム雑音の発生間隔をパルスのオン・オフ時間とすると、その割合を均等にすることができる。

**【0019】**

また、本発明の乱数発生装置は、ランダム雑音発生手段を複数用いて合成したランダム雑音をランダムパルス波生成手段に入力してランダムパルス波のオン・オフの発生頻度を増大させる。

従って、本発明によれば、ランダムパルス波をサンプリングして生成する2値パルス列の周波数をランダムパルス波のオン・オフの発生頻度に応じて高くできるので、乱数の発生をより高速化できる。

**【0020】**

また、本発明の乱数発生装置は、ランダムパルス波生成手段を対数増幅器とコンパレータおよび単安定マルチバイブレータまたはトグルフリップフロップで構成する。

また、2値パルス列符号平滑化手段をクロックの周波数を1/2に分周する1/2分周器とマルチプレクサまたはXORゲートで構成する。

**【0021】**

従って、本発明によれば、デジタル回路を主体に装置を構成できるので、微弱信号を扱うアナログ回路の部分が少なくなり、外乱などの影響を受け難くなって装置の信頼性が向上する。

また、回路が簡素化され、アナログ的な調整もほとんど不要になるので、製造コストを低減すると共に、量産化も容易になる。

**【図面の簡単な説明】****【図1】**

本発明を実施した乱数発生装置のブロック図である。

**【図2】**

図1の各ブロックの信号波形とそのタイミングチャートである。

**【図3】**

本発明を実施したサンプル&ホールド回路の論理図である。

**【図4】**

本発明を実施した分周器の論理図の変形例である。

**【図5】**

本発明を実施したスイッチング回路の論理図である。

【図 6】

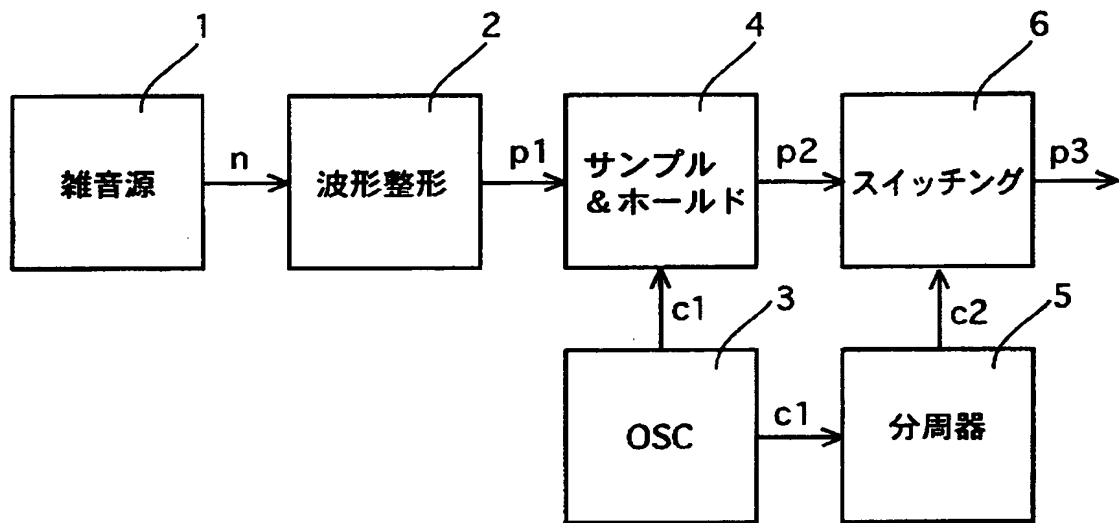
本発明を実施したスイッチング回路の論理図の変形例である。

【符号の説明】

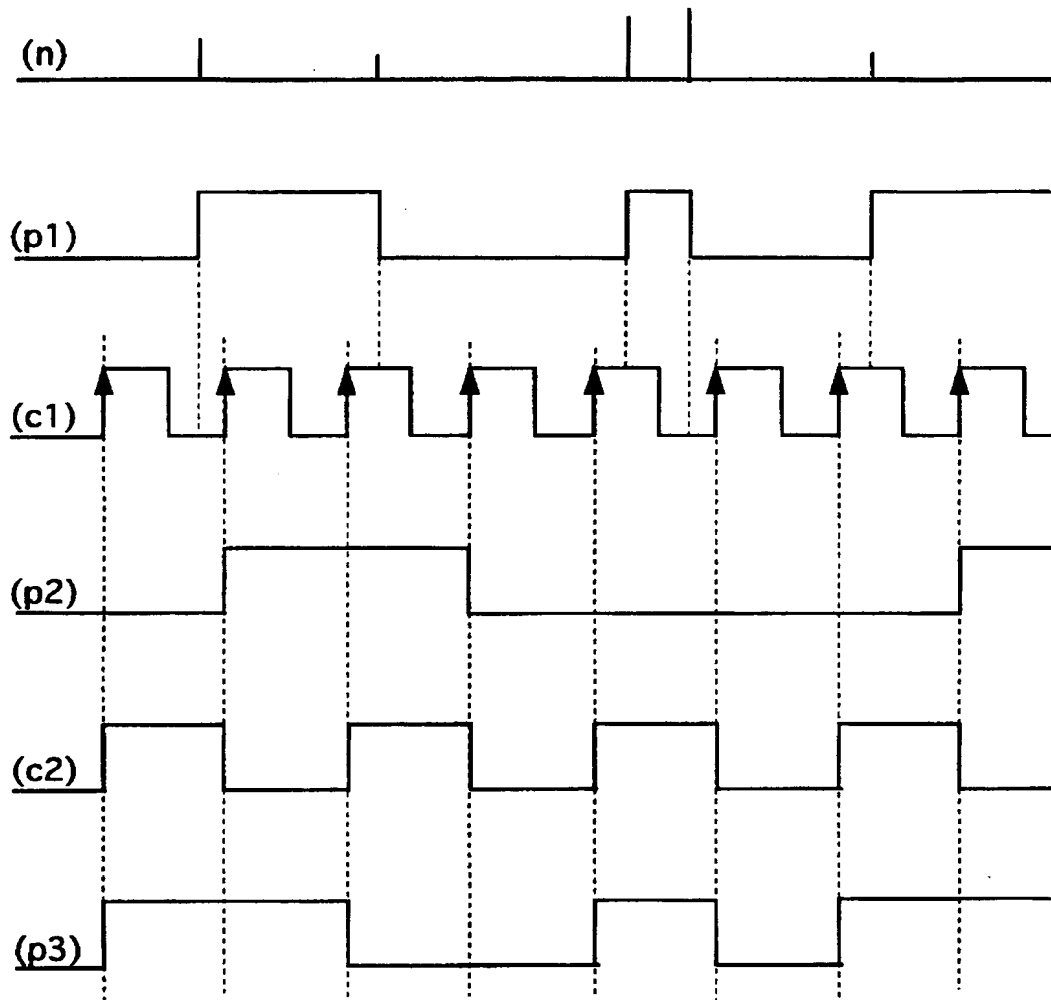
- 1 雑音源
- 2 波形整形回路
- 3 発振器
- 4 サンプル&ホールド回路
- 5 分周器
- 6 スwitching回路

【書類名】 図面

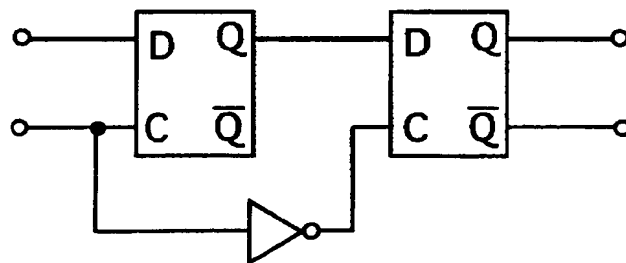
【図 1】



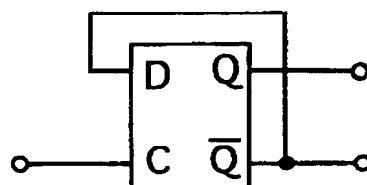
【図 2】



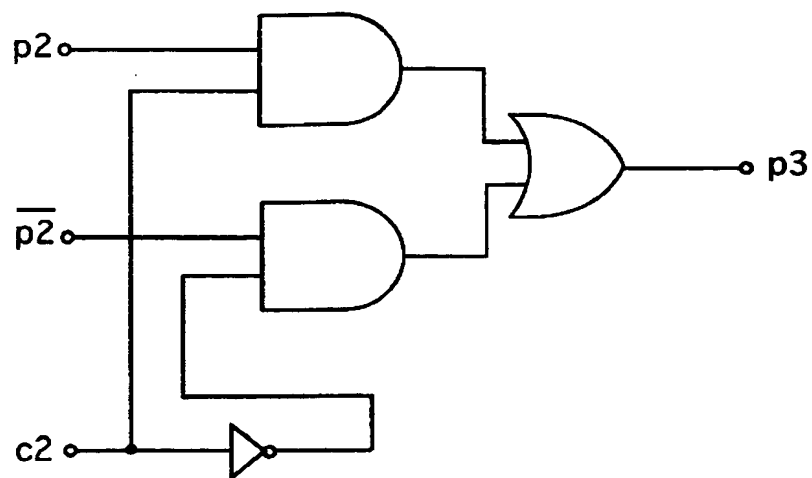
【図 3】



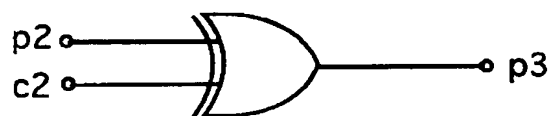
【図 4】



【図 5】



【図 6】



【書類名】 要約書

【要約】

【課題】 偶然性に支配されることなく物理乱数のインバランスを解消して確実に 1 / 0 の出現バランスを等確率にできる乱数発生装置を提供する。

【解決手段】 雑音源 1 が発生する周期性のないランダム雑音 n を波形整形回路 2 に入力してランダムパルス波 p 1 を生成し、次に、ランダムパルス波 p 1 と発振器 3 のクロック c 1 をサンプル&ホールド回路 4 に入力して一定周期の 2 値パルス列 p 2 を生成し、その 2 値パルス列 p 2 とクロック c 1 を分周器 5 で 1 / 2 に分周した 1 / 2 分周クロック c 2 をスイッチング回路 6 に入力して 2 値パルス列 p 2 の極性を 1 周期おきに反転させ、 1 / 0 符号の出現バランスを平滑化した平滑 2 値パルス列 p 3 を出力する。

【選択図】 図 1



特願 2 0 0 1 - 1 6 3 4 2 8

出 願 人 履 歴 情 報

識別番号 [ 5 9 5 0 9 5 3 5 3 ]

1. 変更年月日 1 9 9 7 年 1 2 月 8 日

[変更理由] 住所変更

住 所 神奈川県横浜市都筑区池辺町字山王前 4 5 0 9 番地

氏 名 株式会社三技協

特願 2 0 0 1 - 1 6 3 4 2 8

出 願 人 履 歴 情 報

識別番号 [ 5 0 0 4 5 9 2 9 2 ]

1. 変更年月日 2 0 0 0 年 8 月 2 8 日

[変更理由] 新規登録

住 所 神奈川県相模原市北里 2 - 1 7 - 2 7

氏 名 株式会社サンテクト